We claim:

1. A computer-implemented method for authenticating a user to one or more groups, said method comprising the steps of:

computationally verifying an identity of said user; and

computationally verifying a membership of said user with said one or more groups, wherein said verifying computations are performed substantially simultaneously using user information stored in a computer file associated with said user.

2. The method of claim 1, further comprising the step of registering said user with at least one of said one or more groups.

3. The method of claim 2, wherein said registering step further comprises the step of said user and said at least one of said one or more groups exchanging a respective identifier.

4. The method of claim 3, wherein said user identifier is expressed as follows:

$ID_i = g^{x_i h} \bmod p$,

where g and x_i are randomly generated numbers, and h is a hash function on a random number concatenated with information of said user, U.

5. The method of claim 3, wherein said identifier of said at least one of said one or more groups is expressed as follows:

$G_i = g^{k_i h} \bmod p$,

where g and k_i are randomly generated numbers, and h is a hash function on a random number concatenated with information of said user, U.

6. The method of claim 2, wherein said registering step further comprises the step of creating a registration identifier.

7. The method of claim 6, wherein said registering step between said user, U, and said at least one of said one or more groups, G_i, further comprises the step of creating a registration identifier, (G_i, S_i), where $(S_i = g^{si})$, g is a randomly generated number and s_i is obtained as follows:

$$s_t = x_t h - k_i hG \bmod (p-1).$$

8. The method of claim 1, wherein said user identity and membership are verified if:

$$G^G g^{V(r,s)} \stackrel{?}{=} \prod_{i=1}^{l} ID_i g^r \text{ , mod p.}$$

wherein said user is identified by an identifier, ID_i, equal to $g^{x_i h}$ mod p, said one or more groups are identified by an identifier, G_i, equal to $g^{k_i h}$, $V(r,s) = \sum_{i=1}^{l} s_t + r$, r is a randomly selected wrap value, mod p, g and x_i are randomly generated numbers, h is a hash function on a random number concatenated with user information and s_i is obtained as follows:

$$s_i = x_i h - k_i hG \bmod (p-1).$$

9. The method of claim 1, wherein said verifying computations are performed in a single operation based on the El Gomal public key algorithm.

10. The method of claim 1, wherein said user information is stored on a smart card that provides tamper-resistant features.

11. The method of claim 1, wherein said user information is stored in a memory of a computer.

12. The method of claim 1, wherein a user that satisfies said verifying computations is allowed to access a plurality of groups.

13. A method for authenticating a user to one or more groups, said method comprising the steps of:

verifying an identity of said user; and

verifying a membership of said user with said one or more groups, wherein said verifying steps are performed using a single operation.

14. The method of claim 13, further comprising the step of registering said user with at least one of said one or more groups.

15. The method of claim 14, wherein said registering step further comprises the step of said user and said at least one of said one or more groups exchanging a respective identifier.

16. The method of claim 15, wherein said user identifier is expressed as follows:

$ID_i = g^{x_i h} \bmod p$,

where g and x_i are randomly generated numbers, and h is a hash function on a random number concatenated with information of said user, U.

17. The method of claim 15, wherein said identifier of said at least one of said one or more groups is expressed as follows:

$G_i = g^{k_i h} \bmod p$,

where g and k_i are randomly generated numbers, and h is a hash function on a random number concatenated with information of said user, U.

18. The method of claim 13, wherein said single operation is expressed as:

$$G^G g^{V(r,s)} \stackrel{?}{=} \prod_{i=1}^{l} ID_i g^r \text{, mod p,}$$

and wherein said user is identified by an identifier, ID_i, equal to $g^{x_i h} \bmod p$, said one or more groups are identified by an identifier, G_i, equal to $g^{k_i h}$, $V(r,s)=\sum_{i=1}^{l} s_i + r$, r is a randomly selected

wrap value, mod p, g and x_i are randomly generated numbers, h is a hash function on a random number concatenated with user information and s_i is obtained as follows:

$$s_t = x_t h - k_t hG \bmod (p-1).$$

19. The method of claim 13, wherein said single operation is based on the El Gomal public key algorithm.

20. The method of claim 13, wherein said single operation processes user information stored on a smart card that provides tamper-resistant features.

21. The method of claim 13, wherein said single operation processes user information stored in a memory of a computer.

22. A system for authenticating a user to one or more groups, said system comprising:

a memory that stores computer-readable code; and

a processor operatively coupled to said memory, said processor configured to implement said computer-readable code, said computer-readable code configured to:

verify an identity of said user; and

verify a membership of said user with said one or more groups, wherein said verifying computations are performed substantially simultaneously using user information stored in a computer file associated with said user.

23. An article of manufacture for authenticating a user to one or more groups, comprising:

a computer readable medium having computer readable code means embodied thereon, said computer readable program code means comprising:

a step to verify an identity of said user; and

a step to verify a membership of said user with said one or more groups, wherein said verifying computations are performed substantially simultaneously using user information stored in a computer file associated with said user.

24. A system for authenticating a user to one or more groups, said method comprising the steps of:

a memory that stores computer-readable code; and

a processor operatively coupled to said memory, said processor configured to implement said computer-readable code, said computer-readable code configured to:

verify an identity of said user; and

verify a membership of said user with said one or more groups, wherein said verifying steps are performed using a single operation.

25. An article of manufacture for authenticating a user to one or more groups, comprising:

a computer readable medium having computer readable code means embodied thereon, said computer readable program code means comprising:

a step to verify an identity of said user; and

a step to verify a membership of said user with said one or more groups, wherein said verifying steps are performed using a single operation.